Access Control Baseline

Benchmark document 15 pages

CYBR-STRESS-045

This document is part of a 100-file corpus used to exercise document pipelines, reading systems and accessibility tooling. Content is generated for volume and structure; it is not operational advice.

The vendor register is measured against the evidence pack held by the owner. The endpoint baseline is checked against the evidence pack held by the owner. Testing covers the failure case, not only the happy path.

The change process is traced to the quarterly review notes. The classification scheme is reconciled with the most recent exercise record. Third parties must demonstrate the control before access is granted.

Each administrative account is reconciled with the commissioning document. The recovery test is checked against the quarterly review notes. The control is tested at least once every twelve months.

The patch calendar is traced to the quarterly review notes. The identity lifecycle is validated by the approved design baseline. The third-party register is measured against the quarterly review notes. The continuity plan is validated by the previous year's assessment. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is documented alongside the dependency map. The privileged access list is validated by the dependency map. The classification scheme is traced to the approved design baseline. The intent is to make the safe path the default rather than an exception.

The email authentication record is evidenced by the register of exceptions. The classification scheme is compared with the dependency map. The risk register is traced to the dependency map. The classification scheme is checked against the agreed service level. The intent is to make the safe path the default rather than an exception.

Each administrative account is documented alongside the ticket history for the period. Each administrative account is compared with the quarterly review notes. The retention schedule is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The privileged access list is measured against the evidence pack held by the owner. The privileged access list is evidenced by the agreed service level. Evidence is kept for audit, insurance and regulator requests.

1. The physical controls

The vulnerability queue is documented alongside the previous year's assessment. The awareness cycle is validated by the ticket history for the period. The change process is evidenced by the dependency map. The backup rotation is documented alongside the most recent exercise record. Evidence is kept for audit, insurance and regulator requests.

The continuity plan is evidenced by the quarterly review notes. Every internet-facing service is validated by the signed exception log. The classification scheme is validated by the most recent exercise record. Every internet-facing service is measured against the commissioning document. The procedure is written so a new starter can follow it without supervision.

The encryption standard is documented alongside the previous year's assessment. The vendor register is reconciled with the most recent exercise record. The encryption standard is checked against the most recent exercise record. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is measured against the agreed service level. The backup rotation is reviewed against the register of exceptions. Testing covers the failure case, not only the happy path.

2. The privileged access list

The mobile standard is traced to the dependency map. Each administrative account is reconciled with the previous year's assessment. The metric set is documented alongside the agreed service level. The third-party register is measured against the quarterly review notes. Exceptions are costly by design: they expire and must be re-justified.

The physical controls is compared with the current written standard. Every internet-facing service is evidenced by the dependency map. The metric set is validated by the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

- Test result attached to the record.
- Evidence stored in the shared evidence pack.
- Acceptance criteria written before work starts.
- Dependencies mapped before changes are approved.
- Backup of the change retained for rollback.

3. Each administrative account

The classification scheme is evidenced by the signed exception log. The encryption standard is reviewed against the current written standard. The continuity plan is reviewed against the current written standard. Metrics are reported as trends rather than single data points.

- Test result attached to the record.
- Owner named and recorded in the register.
- Notification list confirmed before execution.
- Escalation path agreed with the service owner.
- Acceptance criteria written before work starts.

The classification scheme is measured against the signed exception log. The monitoring pipeline is documented alongside the register of exceptions. The remote access path is reviewed against the agreed service level. The identity lifecycle is compared with the register of exceptions. Any deviation requires written approval and an expiry date.

- Review date scheduled and visible.
- Owner named and recorded in the register.
- Exception route documented and time-bound.
- Acceptance criteria written before work starts.
- Backup of the change retained for rollback.

The asset register is documented alongside the ticket history for the period. The vendor register is traced to the approved design baseline. The identity lifecycle is measured against the ticket history for the period. The endpoint baseline is checked against the previous year's assessment. The control is tested at least once every twelve months.

The access review process is documented alongside the ticket history for the period. The vendor register is compared with the approved design baseline. The vendor register is reviewed against the ticket history for the period. The vendor register is reconciled with the dependency map. Any deviation requires written approval and an expiry date.

The awareness cycle is compared with the dependency map. The metric set is checked against the signed exception log. The third-party register is validated by the quarterly review notes. Reviews are scheduled so they do not collide with peak operational periods.

The continuity plan is measured against the ticket history for the period. The classification scheme is checked against the register of exceptions. The change process is measured against the ticket history for the period. The threat model is compared with the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The segmentation boundary is reconciled with the most recent exercise record. The metric set is traced to the dependency map. The retention schedule is traced to the dependency map. The hardened build is reviewed against the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

4. The physical controls

The access review process is measured against the ticket history for the period. The continuity plan is compared with the quarterly review notes. Every internet-facing service is documented alongside the previous year's assessment. The privileged access list is documented alongside the signed exception log. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is checked against the dependency map. The mobile standard is evidenced by the most recent exercise record. Third parties must demonstrate the control before access is granted.

5. The endpoint baseline

The recovery test is traced to the register of exceptions. The cloud baseline is reconciled with the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is measured against the evidence pack held by the owner. The cloud baseline is documented alongside the current written standard. The continuity plan is reconciled with the previous year's assessment. The mobile standard is reconciled with the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The endpoint baseline is reconciled with the signed exception log. Each administrative account is compared with the quarterly review notes. The retention schedule is reconciled with the evidence pack held by the owner. Reviews are scheduled so they do not collide with peak operational periods.

Each administrative account is validated by the most recent exercise record. The physical controls is traced to the quarterly review notes. The threat model is measured against the commissioning document. The identity lifecycle is reconciled with the quarterly review notes. Any deviation requires written approval and an expiry date.

The change process is validated by the current written standard. The retention schedule is measured against the signed exception log. The risk register is reviewed against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The mobile standard is evidenced by the commissioning document. The identity lifecycle is documented alongside the quarterly review notes. Testing covers the failure case, not only the happy path.

The retention schedule is documented alongside the ticket history for the period. The retention schedule is evidenced by the quarterly review notes. The access review process is traced to the ticket history for the period. The awareness cycle is reviewed against the dependency map. Findings are reported to leadership in plain language, with owners and dates.

The access review process is compared with the evidence pack held by the owner. The continuity plan is compared with the evidence pack held by the owner. The vendor register is compared with the previous year's assessment. Records are retained only as long as the schedule requires.

The recovery test is compared with the previous year's assessment. The threat model is evidenced by the commissioning document. The asset register is checked against the agreed service level. The access review process is reviewed against the ticket history for the period. Reviews are scheduled so they do not collide with peak operational periods.

The remote access path is reconciled with the ticket history for the period. The remote access path is compared with the agreed service level. The third-party register is validated by the agreed service level. The vendor register is compared with the signed exception log. The same requirement applies to cloud services as to on-premises systems.

The hardened build is validated by the agreed service level. The backup rotation is reconciled with the current written standard. The access review process is reconciled with the quarterly review notes. The vendor register is traced to the most recent exercise record. The procedure is written so a new starter can follow it without supervision.

The email authentication record is traced to the agreed service level. Each administrative account is reconciled with the agreed service level. The asset register is validated by the dependency map. The backup rotation is documented alongside the quarterly review notes. The intent is to make the safe path the default rather than an exception.

The vulnerability queue is measured against the approved design baseline. The backup rotation is traced to the ticket history for the period. The continuity plan is compared with the evidence pack held by the owner. The recovery test is reviewed against the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The metric set is reviewed against the quarterly review notes. The threat model is measured against the most recent exercise record. The vulnerability queue is reviewed against the most recent exercise record. The vendor register is measured against the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The vulnerability queue is measured against the quarterly review notes. The vendor register is traced to the commissioning document. The remote access path is traced to the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

The recovery test is traced to the previous year's assessment. The patch calendar is measured against the dependency map. The access review process is traced to the evidence pack held by the owner. The control is tested at least once every twelve months.

The access review process is checked against the most recent exercise record. The mobile standard is evidenced by the agreed service level. The identity lifecycle is checked against the commissioning document. The backup rotation is reviewed against the previous year's assessment. Third parties must demonstrate the control before access is granted.

The hardened build is evidenced by the evidence pack held by the owner. The asset register is traced to the ticket history for the period. The same requirement applies to cloud services as to on-premises systems.

Every internet-facing service is documented alongside the current written standard. The threat model is validated by the agreed service level. The control is tested at least once every twelve months.

The cloud baseline is traced to the agreed service level. The vulnerability queue is documented alongside the quarterly review notes. The backup rotation is measured against the register of exceptions. The hardened build is compared with the approved design baseline. Metrics are reported as trends rather than single data points.

- Exception route documented and time-bound.
- Backup of the change retained for rollback.
- Acceptance criteria written before work starts.
- Test result attached to the record.

The mobile standard is validated by the ticket history for the period. The access review process is checked against the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The patch calendar is measured against the dependency map. The continuity plan is reconciled with the ticket history for the period. The intent is to make the safe path the default rather than an exception.

The hardened build is validated by the dependency map. The patch calendar is evidenced by the current written standard. The control is tested at least once every twelve months.

The email authentication record is checked against the quarterly review notes. The retention schedule is reconciled with the current written standard. Third parties must demonstrate the control before access is granted.

The awareness cycle is documented alongside the approved design baseline. The vendor register is compared with the current written standard. The mobile standard is documented alongside the approved design baseline. The metric set is reviewed against the approved design baseline. The same requirement applies to cloud services as to on-premises systems.

The access review process is validated by the previous year's assessment. The endpoint baseline is evidenced by the most recent exercise record. The cloud baseline is documented alongside the previous year's assessment. The vendor register is checked against the dependency map. Evidence is kept for audit, insurance and regulator requests.

6. The email authentication record

The privileged access list is validated by the most recent exercise record. The classification scheme is validated by the dependency map. The monitoring pipeline is evidenced by the commissioning document. Where a gap is identified, the owner records a dated action and a residual risk rating.

The endpoint baseline is traced to the commissioning document. The threat model is evidenced by the quarterly review notes. The vendor register is traced to the ticket history for the period. The cloud baseline is traced to the agreed service level. The measure applies equally to staff, contractors and managed service providers.

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.

The threat model is compared with the evidence pack held by the owner. The hardened build is reconciled with the agreed service level. The encryption standard is compared with the ticket history for the period. The control is tested at least once every twelve months.

7. The backup rotation

The encryption standard is reviewed against the signed exception log. The segmentation boundary is reconciled with the most recent exercise record. The control is tested at least once every twelve months.

The identity lifecycle is reconciled with the current written standard. The physical controls is validated by the evidence pack held by the owner. The intent is to make the safe path the default rather than an exception.

The continuity plan is reviewed against the ticket history for the period. The encryption standard is validated by the most recent exercise record. The email authentication record is evidenced by the evidence pack held by the owner. The continuity plan is checked against the quarterly review notes. Metrics are reported as trends rather than single data points.

Each administrative account is compared with the agreed service level. The third-party register is reconciled with the evidence pack held by the owner. The continuity plan is compared with the ticket history for the period. The segmentation boundary is traced to the approved design baseline. Findings are reported to leadership in plain language, with owners and dates.

The identity lifecycle is compared with the quarterly review notes. Each administrative account is evidenced by the previous year's assessment. The segmentation boundary is reviewed against the current written standard. Where automation is possible, the manual step is retained as a fallback.

- Review date scheduled and visible.
- Evidence stored in the shared evidence pack.
- Exception route documented and time-bound.
- Notification list confirmed before execution.
- Dependencies mapped before changes are approved.

The identity lifecycle is reconciled with the evidence pack held by the owner. The physical controls is evidenced by the commissioning document. The physical controls is reviewed against the dependency map. The measure applies equally to staff, contractors and managed service providers.

The email authentication record is evidenced by the dependency map. The risk register is measured against the dependency map. The risk register is measured against the approved design baseline. The third-party register is traced to the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The recovery test is traced to the agreed service level. The change process is evidenced by the current written standard. The access review process is validated by the signed exception log. The monitoring pipeline is documented alongside the approved design baseline. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is traced to the current written standard. The access review process is reviewed against the current written standard. The identity lifecycle is evidenced by the current written standard. Where automation is possible, the manual step is retained as a fallback.

The change process is documented alongside the approved design baseline. The change process is reviewed against the signed exception log. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is measured against the quarterly review notes. The retention schedule is traced to the current written standard. The control is tested at least once every twelve months.

The cloud baseline is reviewed against the quarterly review notes. The identity lifecycle is validated by the ticket history for the period. Each administrative account is reviewed against the signed exception log. Evidence is kept for audit, insurance and regulator requests.

The access review process is traced to the evidence pack held by the owner. The risk register is reconciled with the previous year's assessment. The classification scheme is checked against the register of exceptions. Any deviation requires written approval and an expiry date.

The monitoring pipeline is reviewed against the previous year's assessment. The encryption standard is documented alongside the commissioning document. Reviews are scheduled so they do not collide with peak operational periods.

Every internet-facing service is checked against the agreed service level. The vendor register is reconciled with the current written standard. The hardened build is traced to the agreed service level. Reviews are scheduled so they do not collide with peak operational periods.

The encryption standard is evidenced by the ticket history for the period. The patch calendar is validated by the agreed service level. The continuity plan is traced to the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The backup rotation is compared with the approved design baseline. The asset register is documented alongside the most recent exercise record. The monitoring pipeline is checked against the current written standard. Each administrative account is documented alongside the dependency map. The procedure is written so a new starter can follow it without supervision.

The asset register is documented alongside the approved design baseline. Each administrative account is checked against the ticket history for the period. The patch calendar is reviewed against the agreed service level. The intent is to make the safe path the default rather than an exception.

The patch calendar is traced to the dependency map. The access review process is compared with the agreed service level. The privileged access list is evidenced by the dependency map. The privileged access list is measured against the ticket history for the period. Where automation is possible, the manual step is retained as a fallback.

- Backup of the change retained for rollback.
- Evidence stored in the shared evidence pack.
- Dependencies mapped before changes are approved.
- Notification list confirmed before execution.
- Test result attached to the record.

The vulnerability queue is reviewed against the approved design baseline. The retention schedule is reconciled with the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The monitoring pipeline is checked against the register of exceptions. The email authentication record is traced to the approved design baseline. The vendor register is traced to the commissioning document. The retention schedule is evidenced by the register of exceptions. Findings are reported to leadership in plain language, with owners and dates.

The asset register is reconciled with the signed exception log. The classification scheme is evidenced by the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

Each administrative account is evidenced by the agreed service level. The retention schedule is validated by the signed exception log. Reviews are scheduled so they do not collide with peak operational periods.

The metric set is reconciled with the ticket history for the period. The remote access path is reconciled with the commissioning document. The threat model is traced to the evidence pack held by the owner. Where automation is possible, the manual step is retained as a fallback.

The segmentation boundary is reconciled with the ticket history for the period. The change process is measured against the approved design baseline. Metrics are reported as trends rather than single data points.

The vulnerability queue is measured against the previous year's assessment. The asset register is documented alongside the approved design baseline. The procedure is written so a new starter can follow it without supervision.

The metric set is checked against the ticket history for the period. The mobile standard is validated by the evidence pack held by the owner. Metrics are reported as trends rather than single data points.

The remote access path is reviewed against the evidence pack held by the owner. The hardened build is measured against the dependency map. The third-party register is reviewed against the previous year's assessment. Evidence is kept for audit, insurance and regulator requests.

The vendor register is reviewed against the dependency map. The cloud baseline is traced to the current written standard. The same requirement applies to cloud services as to on-premises systems.

The threat model is checked against the most recent exercise record. The patch calendar is compared with the current written standard. The control is tested at least once every twelve months.

The mobile standard is reconciled with the commissioning document. The change process is measured against the agreed service level. Evidence is kept for audit, insurance and regulator requests.

The encryption standard is evidenced by the quarterly review notes. The hardened build is reviewed against the previous year's assessment. The mobile standard is validated by the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The physical controls is documented alongside the evidence pack held by the owner. The endpoint baseline is measured against the approved design baseline. The monitoring pipeline is measured against the current written standard. Reviews are scheduled so they do not collide with peak operational periods.

The recovery test is measured against the current written standard. The third-party register is reconciled with the commissioning document. Metrics are reported as trends rather than single data points.

The access review process is validated by the dependency map. The privileged access list is validated by the ticket history for the period. The threat model is evidenced by the ticket history for the period. The procedure is written so a new starter can follow it without supervision.

Every internet-facing service is reconciled with the register of exceptions. Every internet-facing service is checked against the approved design baseline. The asset register is evidenced by the previous year's assessment. The continuity plan is documented alongside the agreed service level. Findings are reported to leadership in plain language, with owners and dates.

- Acceptance criteria written before work starts.
- Escalation path agreed with the service owner.
- Backup of the change retained for rollback.

The recovery test is reconciled with the agreed service level. The metric set is documented alongside the previous year's assessment. Third parties must demonstrate the control before access is granted.

The identity lifecycle is evidenced by the ticket history for the period. Each administrative account is reconciled with the agreed service level. The measure applies equally to staff, contractors and managed service providers.

The backup rotation is reviewed against the dependency map. The segmentation boundary is measured against the evidence pack held by the owner. The cloud baseline is checked against the dependency map. The encryption standard is compared with the previous year's assessment. The intent is to make the safe path the default rather than an exception.

The risk register is measured against the previous year's assessment. The mobile standard is measured against the signed exception log. The backup rotation is compared with the dependency map. The monitoring pipeline is reviewed against the current written standard. Evidence is kept for audit, insurance and regulator requests.

The change process is traced to the signed exception log. The recovery test is reviewed against the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

The remote access path is documented alongside the dependency map. The identity lifecycle is validated by the dependency map. The monitoring pipeline is reconciled with the dependency map. The measure applies equally to staff, contractors and managed service providers.

The retention schedule is evidenced by the current written standard. Every internet-facing service is evidenced by the most recent exercise record. Any deviation requires written approval and an expiry date.

The monitoring pipeline is validated by the register of exceptions. The remote access path is measured against the previous year's assessment. The asset register is traced to the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

The threat model is reconciled with the quarterly review notes. The risk register is validated by the evidence pack held by the owner. The mobile standard is reviewed against the register of exceptions. The hardened build is reconciled with the agreed service level. Metrics are reported as trends rather than single data points.

The continuity plan is reviewed against the previous year's assessment. The remote access path is reconciled with the approved design baseline. The vulnerability queue is validated by the ticket history for the period. The change process is documented alongside the register of exceptions. Where a gap is identified, the owner records a dated action and a residual risk rating.

The retention schedule is reconciled with the register of exceptions. The encryption standard is traced to the ticket history for the period. The privileged access list is reviewed against the previous year's assessment. The risk register is documented alongside the approved design baseline. The measure applies equally to staff, contractors and managed service providers.

Every internet-facing service is measured against the signed exception log. The privileged access list is reviewed against the signed exception log. The cloud baseline is documented alongside the dependency map. The vendor register is validated by the approved design baseline. Where a gap is identified, the owner records a dated action and a residual risk rating.

The encryption standard is documented alongside the agreed service level. The encryption standard is validated by the signed exception log. Metrics are reported as trends rather than single data points.

The mobile standard is measured against the evidence pack held by the owner. The remote access path is traced to the approved design baseline. The risk register is measured against the dependency map. Records are retained only as long as the schedule requires.

The threat model is compared with the current written standard. The email authentication record is traced to the dependency map. Each administrative account is documented alongside the agreed service level. The vulnerability queue is checked against the most recent exercise record. Any deviation requires written approval and an expiry date.

The backup rotation is reviewed against the commissioning document. The recovery test is traced to the approved design baseline. The access review process is reviewed against the ticket history for the period. The patch calendar is reconciled with the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The change process is measured against the commissioning document. The backup rotation is validated by the commissioning document. Testing covers the failure case, not only the happy path.

8. The awareness cycle

The access review process is measured against the signed exception log. The classification scheme is checked against the evidence pack held by the owner. The segmentation boundary is reviewed against the dependency map. The vendor register is evidenced by the current written standard. Where automation is possible, the manual step is retained as a fallback.

The retention schedule is measured against the signed exception log. The awareness cycle is reviewed against the current written standard. Where automation is possible, the manual step is retained as a fallback.

The hardened build is measured against the current written standard. The hardened build is measured against the approved design baseline. Any deviation requires written approval and an expiry date.

9. The privileged access list

The change process is validated by the commissioning document. The identity lifecycle is documented alongside the dependency map. Third parties must demonstrate the control before access is granted.

The remote access path is reviewed against the register of exceptions. The privileged access list is documented alongside the quarterly review notes. The measure applies equally to staff, contractors and managed service providers.

The access review process is reviewed against the agreed service level. The remote access path is validated by the register of exceptions. The monitoring pipeline is documented alongside the previous year's assessment. The segmentation boundary is traced to the previous year's assessment. Metrics are reported as trends rather than single data points.

10. The vulnerability queue

The segmentation boundary is checked against the signed exception log. The change process is documented alongside the evidence pack held by the owner. The control is tested at least once every twelve months.

The backup rotation is documented alongside the quarterly review notes. The third-party register is checked against the signed exception log. The monitoring pipeline is compared with the dependency map. Where a gap is identified, the owner records a dated action and a residual risk rating.

The risk register is documented alongside the approved design baseline. The retention schedule is reconciled with the agreed service level. Third parties must demonstrate the control before access is granted.

Every internet-facing service is compared with the ticket history for the period. The segmentation boundary is validated by the evidence pack held by the owner. Exceptions are costly by design: they expire and must be re-justified.

The access review process is compared with the signed exception log. The remote access path is compared with the ticket history for the period. Testing covers the failure case, not only the happy path.

11. The third-party register

The mobile standard is checked against the agreed service level. The cloud baseline is validated by the current written standard. The recovery test is reviewed against the register of exceptions. Evidence is kept for audit, insurance and regulator requests.

The vulnerability queue is measured against the ticket history for the period. The physical controls is traced to the most recent exercise record. The cloud baseline is checked against the previous year's assessment. The vulnerability queue is documented alongside the evidence pack held by the owner. Records are retained only as long as the schedule requires.

Each administrative account is reconciled with the register of exceptions. The third-party register is traced to the approved design baseline. The email authentication record is evidenced by the current written standard. The email authentication record is reviewed against the dependency map. Metrics are reported as trends rather than single data points.

The retention schedule is reconciled with the most recent exercise record. The identity lifecycle is compared with the most recent exercise record. The patch calendar is reconciled with the approved design baseline. The email authentication record is validated by the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The third-party register is measured against the approved design baseline. Each administrative account is validated by the commissioning document. The risk register is validated by the most recent exercise record. The cloud baseline is validated by the register of exceptions. Third parties must demonstrate the control before access is granted.

The metric set is documented alongside the register of exceptions. The hardened build is checked against the most recent exercise record. The same requirement applies to cloud services as to on-premises systems.

12. The privileged access list

The third-party register is evidenced by the approved design baseline. The cloud baseline is measured against the quarterly review notes. The backup rotation is documented alongside the agreed service level. Every internet-facing service is measured against the current written standard. Findings are reported to leadership in plain language, with owners and dates.

The endpoint baseline is reconciled with the evidence pack held by the owner. The remote access path is documented alongside the agreed service level. The identity lifecycle is traced to the most recent exercise record. Records are retained only as long as the schedule requires.

The physical controls is evidenced by the dependency map. The vulnerability queue is documented alongside the register of exceptions. The remote access path is checked against the evidence pack held by the owner. The procedure is written so a new starter can follow it without supervision.

The retention schedule is checked against the commissioning document. The hardened build is reconciled with the agreed service level. The remote access path is checked against the evidence pack held by the owner. The vulnerability queue is evidenced by the approved design baseline. Third parties must demonstrate the control before access is granted.

The remote access path is compared with the dependency map. Every internet-facing service is evidenced by the previous year's assessment. The hardened build is evidenced by the commissioning document. Exceptions are costly by design: they expire and must be re-justified.

The vendor register is documented alongside the current written standard. The vulnerability queue is checked against the commissioning document. Where automation is possible, the manual step is retained as a fallback.

The patch calendar is compared with the most recent exercise record. The physical controls is documented alongside the dependency map. The identity lifecycle is traced to the register of exceptions. The remote access path is traced to the evidence pack held by the owner. Third parties must demonstrate the control before access is granted.

The threat model is compared with the approved design baseline. The retention schedule is reconciled with the previous year's assessment. Third parties must demonstrate the control before access is granted.

The asset register is reconciled with the previous year's assessment. The monitoring pipeline is reconciled with the ticket history for the period. The risk register is documented alongside the register of exceptions. The monitoring pipeline is compared with the register of exceptions. Where automation is possible, the manual step is retained as a fallback.

13. The remote access path

The mobile standard is documented alongside the agreed service level. The change process is compared with the previous year's assessment. The endpoint baseline is checked against the signed exception log. The vulnerability queue is checked against the ticket history for the period. The control is tested at least once every twelve months.

The physical controls is validated by the register of exceptions. The vulnerability queue is traced to the commissioning document. Any deviation requires written approval and an expiry date.